



Kuntsman, Adi ORCID logoORCID: <https://orcid.org/0000-0002-9970-9866>,
Miyake, Esperanza ORCID logoORCID: <https://orcid.org/0000-0001-5504-7648> and Martin, Samantha (2019) Re-thinking Digital Health: Data, Appisa-
tion and the (im)possibility of 'Opting out'. Digital Health, 5. ISSN 2055-2076

Downloaded from: <https://e-space.mmu.ac.uk/624132/>

Version: Published Version

Publisher: SAGE Publications (UK and US)

DOI: <https://doi.org/10.1177/2055207619880671>

Usage rights: Creative Commons: Attribution-Noncommercial 4.0

Please cite the published version

<https://e-space.mmu.ac.uk>

Re-thinking Digital Health: Data, Appisation and the (im)possibility of ‘Opting out’

Adi Kuntsman , Esperanza Miyake and Sam Martin

Digital Health
Volume 5: 1–16
© The Author(s) 2019
Article reuse guidelines:
sagepub.com/journals-
permissions
DOI: 10.1177/2055207619880671
journals.sagepub.com/home/dhj



Abstract

Presented as providing cost-, time- and labour- effective tools for the (self)management of health, health apps are often celebrated as beneficial to all. However, their negative effects – commodification of user data and infringement on privacy – are rarely addressed. This article focuses on one particularly troubling aspect: the difficulty of opting out of data sharing and aggregation during app use or after unsubscribing/uninstalling the app. Working in the context of the new European General Data Protection Regulation and its implementation in the UK health services, our analysis reveals the discrepancy between the information presented to users, and the apps’ actual handling of user data. We also point to the fundamental tension in the digitisation of health, between the neoliberal model where both health and data concerns are viewed as an individual’s responsibility, and the digital-capitalist model, which puts forward, and capitalises on, collective (‘Big’) data. Pulled between the ‘biopolitics of the self’ and the ‘biopolitics of the population’ (concepts coined by Btihad Ajana), opting out of health datafication therefore cannot be resolved as a matter of individual right alone. The article offers two contributions. Methodologically, we present a toolkit for a multi-level assessment of apps from the perspective of opting out, which can be adapted and used in future research. Conceptually, the article brings together critical digital health scholarship with the perspective of data justice, offering a new approach to health apps, which focuses on *opt-out* as a legal, social and technical possibility, and as a collective citizen and user right.

Keywords

Health apps, datafication, data justice, GDPR, trust, opting out, data sharing, privacy, surveillance capitalism, biopolitics

Received 1 March 2019; accepted 12 September 2019

Introduction

‘There’s an App for that!’ A catchy Internet phrase of mid 2000s, initiated and subsequently trademarked by Apple, captures what has become an everyday reality for most digital economies. With the widespread use of smartphones, we are increasingly reliant on apps that are either pre-loaded or can be voluntarily/casually and mandatorily/professionally downloaded, to manage all areas of our consumer, work, political and personal lives. The sheer volume, range, speed and breadth of different types of apps available in the market today demonstrate how this all-encompassing ‘appisation’ is now an inevitable part of contemporary digital life.^{1–3} It is impossible to talk about digital health today without referring to appisation (or ‘mHealth’/‘mobile Health’ as the process is more commonly described in medical circles). According to Statista, ‘The health and medical industry have been named as one of the top

three fields to accelerate the growth of mobile devices’.⁴ At present, countless apps are being developed and offered to individual smartphone users to manage healthy lifestyles or to support specific medical and health conditions; the apps are also extensively integrated into public and private health service provisions.^{5,6} However, the invisible yet detrimental by-products of health appisation – such as infringements on privacy, data monetisation and long-term digital profiling – are rarely understood by the medical

Manchester Metropolitan University, Manchester, UK

Corresponding author:

Adi Kuntsman, Room 437, Geoffrey Manton Building, Oxford Road, Manchester, M15 6LL, United Kingdom.
Email: a.kuntsman@mmu.ac.uk
Twitters: Adi Kuntsman @Dr_Ku; Esperanza Miyake @Es_Miyake; Sam Martin @DigitalCoeliac.



Creative Commons Non Commercial CC BY-NC: This article is distributed under the terms of the Creative Commons Attribution-NonCommercial 4.0 License (<http://www.creativecommons.org/licenses/by-nc/4.0/>) which permits non-commercial use, reproduction and distribution of the work without further permission provided the original work is attributed as specified on the SAGE and Open Access pages (<https://us.sagepub.com/en-us/nam/open-access-at-sage>).

practitioners and health service providers advocating for the apps. Nor are these always clear to the users, lured by the speed and convenience of ‘on demand healthcare’, usually advertised as an ‘affordable and accessible service at one’s fingertips’ (to use the words of Babylon Health, one of the leading health apps).⁷ Health appisation is thus presented as an unquestionably positive process, devoid of dangers and beneficial to all – a celebratory framing that both conceals and supports the apps’ data economy of ‘surveillance capitalism’^{8–11} that relies on users’ willing but often unknowing participation and continuous personal ‘contribution’ of their data.

While health appisation may indeed have revolutionised some aspects of healthcare, its broader and often perturbing socio-political effects are yet to be explored in the academic domain of digital health. Deborah Lupton⁵ recently argued that most studies on health apps to date come from medical or public health literature, which focuses primarily on an instrumental approach to apps’ effectiveness or medical validity. What is yet to be interrogated are ‘[t]he wider social, cultural and political roles played by health and medical apps as part of contemporary healthcare and public health practice’⁵ (p. 607) – a task she sets out for ‘critical digital health studies’. In this article, we want to push Lupton’s idea of the critical digital health framework further. We want to challenge some assumptions surrounding the status quo of health app studies by exploring one specific and particularly disturbing aspect of health appisation: not only the surrender of one’s health data, but more worryingly, that once the data is integrated into the apps, there is very little room for *opting out*. In that respect, we approach health apps not just as what Lupton calls ‘socio-cultural artefacts’, but as ‘socio-cultural data traps’, elaborate and sophisticated in their technologies of incorporation and engagement, yet incredibly scarce in social affordances and technical mechanisms for letting go of their ‘data subjects’.

Therefore, the central concern of our article is the question of opt-out as a legal, social and technical possibility, and as a citizen and user right. Our approach aligns with the emerging body of scholarship on ‘data justice’,^{12–15} which, as Linnet Taylor formulates, should include ‘the freedom not to use particular technologies, and in particular not to become part of commercial databases as a by-product of development interventions’¹⁴ (p. 9). Taylor’s framework of data justice was developed when looking at international development, humanitarian intervention, refugee border crossing and population surveillance – in other words, in contexts of precarity and systemic vulnerability, where power and governance increasingly rely on digital data, and where all-encompassing digital

surveillance often manifests as a necessary ‘care’. The leap from here to digital health might seem far-fetched; however we argue that it is precisely the double-bound nature of care versus surveillance that makes the perspective of data justice crucial for critical digital health studies. Because of the intimate relationship between personal health and personal data, which the process of appisation transforms, questions of opting out are of particular urgency to the field of digital health, extending far beyond the domain of the theoretical. In the context of data economies and the continuously increasing appisation of healthcare, these questions are also acute for the general public, medical research bodies and care providers, including private enterprises and national health services. In our discussion, we focus less on the pressure that medical systems put on some patients to use technology as part of their care (for example, apps developed for specific medical conditions). In other words, we are not addressing individual autonomy over choices in medical treatment and management. Rather, our focus is more on the use of health apps generally, understood through the lens of one’s rights to one’s data, beyond the context of medical treatment.

Combining our expertise in digital sociology, cultural studies, digital health, computation and data visualisation, this article aims to make two key contributions to simultaneously advance critical debates in the field of ‘critical digital health studies’ and to inform future research around digitised healthcare. The first contribution lies in our proposed paradigmatic shift from engagement to dis-engagement as a starting point for discussing health appisation (for a broader discussion of ‘digital disengagement’ as a shift in media studies, see Kuntsman and Miyake¹⁶). Current research into digital health, including critical scholarship,^{5,17–20} still largely prioritises *engagement* with digital technologies. Because digital engagement provides access to social networks and health e-resources for individuals, support groups, carers and practitioners, the aim of digital health seems to be – like all other sectors – to make citizen engagement and the digital inseparable from one another. Within such a framework, *disengagement* is envisioned only as an aberration, or an afterthought to be remedied through more tests and trials to increase *engagement*. Such a configuration makes questions of ‘data traps’ and opting out difficult to address beyond instrumental questions of how ‘data management’ or ‘privacy protection’ can be improved. Using the disengagement paradigm, we call instead to place the discussion of legal, social and technical possibilities to opt out at the centre of the work on health appisation, bringing critical digital health scholarship into much needed conversation within the field of data justice.

Our second contribution is a toolkit for multi-level evaluation of the apps themselves. The evaluation process we propose – which is outlined in more detail in the next section – resembles the ‘app walk through’ method, developed by Light et al., where a critical study of the app involves ‘systematically and forensically step[ping] through the various stages of app registration and entry, everyday use and discontinuation of use’²¹ (p. 881). Yet the uniqueness of our toolkit is that it is grounded in the paradigm of digital disengagement, and as such, differs fundamentally from most methodological approaches to the study of health apps. A substantial portion of current health app studies comes from the abovementioned tendency to normalise engagement, thus mostly investing resources into how the apps work or how they can be improved – whether through app development or changes in user experience.^{22,23} By challenging the norm of digital engagement and by exposing the risks and the traps – rather than the promise and the potential – of health apps, we are laying a path for future research that can productively challenge the ways in which digital technologies are often embraced too quickly and without sustained critical consideration. Our toolkit is thus intended for wider use and it is hoped will benefit academic researchers, health app developers and testers, as well as health practitioners and of course the users themselves.

Context and methods

In this article, we take the UK as a case study to develop and test our toolkit, while also demonstrating the applicability of our framework more broadly. In considering the current socio-legal landscape of digital health and opting out in the UK, we reveal how localised processes regarding opt-out are simultaneously a reflection of nation-specific legal and economic conditions *and* of global concerns, especially as those are understood within the context of Big Data, the algorithmic value of appisation, and the shared practices between multinational corporations and services, benefiting from the circulation of personal data around the world. Within such a formulation, it becomes even more pertinent to find more ways to understand the question of opting out at the level of social norms, legal rights, technical opportunities and everyday praxis.

Between the global data economy and the national/regional data rights

As in many other digital economies, the health sector in the UK is increasingly expecting patients to manage their own health and wellbeing through apps.

As such, health apps are widely offered by private companies and the public sector, including the National Health Service (NHS) and especially NHS Digital, ‘the national information and technology partner to the health and care system’.²⁴ The incorporation of apps into NHS Digital is the latest development in the longer tradition of phone and online patient support, designed to reduce the workload of general practitioners (GPs) and hospitals, and in this sense, it should be understood within a broader context of continuous budget cuts leading to diminishing resources for face-to-face and on-site patient support. At the same time, such developments are also part of the general move towards ‘self-responsibilisation’ for one’s health^{25,26} within the wider Euro-American neoliberal context.

At the time of our study in 2018, two major legal developments took place, pivotal for understanding the current opt-out landscape in the UK. Firstly, the European General Data Protection Regulation (GDPR) came into force in May 2018 and was fully adopted in the UK (despite the uncertainty surrounding the process of Brexit). Unlike the earlier UK Data Protection Law, GDPR moves towards a legal framework that defaults to opt-out rather than opt in. The GDPR’s overall aim is to increase people’s control over their own personal data and ‘to protect all EU citizens from privacy and data breaches in an increasingly data-driven world’.²⁷ For companies and organisations this means obtaining consent for using and retaining customers’ personal data; for the ‘data subject’, it grants more rights to be informed and control how their personal data is used. Secondly and related, in May 2018, NHS Digital launched its national data opt out service in line with GDPR guidelines, aimed to provide ‘a facility for individuals to opt out from the use of their data for research or planning purposes’.²⁸

While opt-out rights are at the heart of GDPR, health apps used in the UK are also part of the global capitalist data economy where such rights are diminishing. How then can we understand a European data protection law and (the limits of) its power in the context of global digital platforms and app companies, not to mention their (equally global) data aggregation? Similarly, what are the impacts and the limits of the NHS policies regarding opt-out, when they actively collaborate with private, commercial, third-party app providers who may abide by different corporate rules? Lastly and most pressingly, how is this complex and at times contradictory information communicated to the current or potential app users, or healthcare providers? These questions, arising from the digital-legal context of appisation in the UK, consequently informed the design and execution of our research.

NHS Digital: safety, trustworthiness, confusion

When we began working on our project, NHS Digital was gradually developing GDPR compliance by updating information and editing its pages, among them, the NHS Apps Library. Launched pre-GDPR in April 2017 to offer ‘*Trusted* digital tools for patients and the public to manage and improve their health’ (emphasis added by authors),²⁹ it moved to a new, temporary Beta version at the time of our research. This NHS Apps Library offers an ‘NHS badge’: a tick that appears next to a given app as a sign that it has undergone the process of ‘Vetting Apps’,³⁰ resulting in apps having either the ‘NHS Approved’ or the ‘Being Tested in the NHS’ badge, respectively. Situated within the online NHS environment, the Library is thus a place where a user/patient can assume the apps offered are indeed to be ‘trusted’ and ‘safe’. The reality of the NHS badge is far more complicated and needs unpacking; what constitutes as ‘safety’ and the processes of ‘approval’ are not as clear or transparent as they may first appear to be. First of all, inclusion in the Library does not in fact automatically mean the apps have already been approved. Having an app listed only requires a simple five-step online application process; any developer can put their app through on completion of their Digital Assessment Questions, regardless of the answers (!).³¹ Granted, some apps might be removed after being tested, but they would still remain listed and ‘live’ (i.e. available to use) in the Library while undergoing the vetting process. Tellingly, at the time of our data collection in summer 2018, out of the 49 apps listed only one had the full NHS Approved badge; four had partial approval, and three were in the process of being tested. Secondly, the notion of ‘safety’ in the verification process only partially includes the safety of *data*. App assessment ensures that the app ‘meets NHS quality standards for clinical effectiveness, safety, usability and accessibility, and has evidence to support its use’; the NHS assesses an app’s ‘safety’ according to ‘both clinical safety and information safety (Information Governance, Privacy and Security)’.³¹ Safety, here, conjoins and conflates the notion of health risk and data risk. But while the discourse of ‘approval’/‘vetting’ institutionalises user trust via safety scaffolding, supposedly built into the process of verification, the idea of data safety and what it might entail when bio data is aggregated and mined by the apps, remains obscure. For example, do the ‘vetted’ apps report their data collection protocols to the NHS? What about the third parties, with which the apps share their users’ data? What is missing in this narrative is a clear distinction between medical and data safety, testing and vetting; and more urgently, a transparent explanation regarding what kind of

different and separate process is involved in ‘approving’ medical safety and data safety of the apps.

Within such a changeable site where information on app safety is both opaque and confusing, what are the possibilities of opting out (for example, if a user realises an app is not as ‘safe’ as it might appear)? The NHS Apps Library does not provide information or guidance about the possibilities of leaving the ‘unsafe’ (or the ‘safe’) apps, once they are installed and activated. The only place where opt-out is mentioned is outside of the Library, on the new National data opt out service by NHS Digital, which allows people to ‘opt out of their confidential patient information being used for research and planning’. The scheme replaces the previous ‘type 2 opt-out’, which required NHS Digital to refrain from sharing a patient’s confidential information for purposes beyond their direct care. Type 1 opt-out referred to requests for not sharing one’s information beyond direct care, placed directly with the GP and one’s local surgery.

Indexed under ‘Systems and Services’ and placed in a long, alphabetised list alongside other medical and administrative services within the NHS, information on opting out is very difficult to find and complicated to execute. Users must confront hurdles of clicking through multiple pages, downloading and emailing forms, or searching for alternatives. Such processes would require digital literacy, time, patience and perseverance – a striking contrast to how opting in is usually communicated in today’s digital environments, where ‘download’, ‘subscribe’ and ‘follow’ buttons are large, immediate and consistently visible.

More importantly, there are no links between the National data opt out service by NHS Digital and the Apps Library: it is unclear whether the NHS digital opt-out refers only to the information collected by GP surgeries and hospitals, or extends to the health apps.

As we can see, there is a worrying gap between the online NHS narrative of health app ‘safety’ and the reality of data safety. But in order to truly understand the sheer complexity, tensions and discrepancies between legal frameworks – such as GDPR or patients’ rights – and the reality of data sharing in health app-isation beyond the discursive levels of data and medical ‘safety’, we need to analyse the actual apps, and their policies and practices more closely. Herein lies the value of our toolkit, which we offer as part of an assessment framework to be used alongside a more contextual analysis of the legal and practical conditions that surround health apps.

Methods

Our app assessment toolkit offers a way to evaluate, separately and in relation to each other, the following

elements: (1) the apps' Terms and Conditions as presented on their platforms/websites and within the apps; (2) the apps' 'permissions' to access other data via one's phone and the tracking of data beyond the app itself; and (3) the way an app handles an opt-out *after* installation and use. The toolkit was developed and tested using three apparently 'safe' apps or apps that were, or appeared to have been at the time of our research analysis, NHS-recommended by either appearing in the NHS Apps Library, or by carrying an NHS-endorsed badge within the Apple and Google app stores: Echo,³² Babylon Health (BH),⁷ and Pregnancy Tracker and Baby App (PTBA).³³ Echo is an NHS-developed prescription management app, which was and continues to be at the time of writing, listed in the NHS Apps Library. BH is a UK-based GP consultation tool that was initially listed in the NHS Apps Library; it has since been removed though continues to be advertised on Apple and Google app stores as allowing to 'see an NHS GP', with links to the NHS Apps Library; and is currently also hosted on the nhs.uk domain.³⁴ PTBA is an US-based pregnancy and foetal/baby tracking app, which was never listed in the Library but described in the app stores as containing 'all health information [that] is approved [and] ... certified by the NHS England Information Standard'.³⁵

Once chosen, these apps were then subject to the following steps over the course of 10 weeks:

- Installation on a Samsung Galaxy running Android and an iPhone running iOS.
- Creation and active use of 'dummy' user profiles to replicate real life conditions as much as possible.
- Installation and adaption of the open source Exodus analytical tools for Android applications (an open source auditing platform with multiple applications, allowing detection of app/device behaviours that may be infringing user privacy through ads, tracking, analytics and listening tools).³⁶ For legal reasons, such tracking is not currently possible for iPhone iOS applications.³⁷ (At the time of writing, Apple's proprietary iOS platform remains a locked digital rights management system, where under the United States DMCA 1201 Law, and European Article 6 of the EUCD, bypassing it constitutes a legal offence leading to imprisonment and a fine; see Doctorow³⁷); the Exodus CLI client for local analysis, and Etip – the Exodus tracker investigation platform.³⁸
- Analysis of network traffic on each app by using the Exodus proxy tool to record which external trackers or third-party servers each app communicated with when used (to determine what types of user data were being collected, and which external third-party servers the data was sent to).³⁹
- Concurrent use of the open source Apktool⁴⁰ to investigate the source code and operating processes of each Android app, to further identify any known trackers (e.g. hidden Facebook and Google Analytics or advertising bots) that might exist in the source code of each app.
- Documenting each tracker or type of data requested, and comparison of the findings with Exodus data reports, paying particular attention to the third parties with which the data was shared, such as Google and Facebook.
- Deactivation of apps on both phones, noting the potential 'opt-out' options, the steps needed to terminate the account, and the relation between deactivation of the app and withdrawal of the data already collected.

Far from using the three apps as a 'representative' sample of a wide range of health apps, we approached them as a testing ground to build our analytical toolkit and related evaluation criteria, both discursive and technical. What we present in the following section is simultaneously an assessment of empirical evidence, and a demonstration of the benefits and uses of our toolkit for future research.

The toolkit

Assessing the apps' Terms and Conditions

Since health apps operate in a field of conflicting legal and social frameworks with regards to data rights and safety, it is important to incorporate these frameworks when assessing the apps' legal communication. For the first element of our toolkit, we integrated three distinct, complementary sets of guidelines:

- Caldicott Principles used in the NHS for handling identifiable patient information,⁴¹ which strictly regulate the process of collecting and storing such information, yet do not refer to how the process is communicated to the patients themselves. The Principles require: justification of the purpose(s) of collecting information; not using patient-identifiable information unless it is necessary; using the minimum necessary patient-identifiable information; limiting access to patient-identifiable information on a strict need-to-know basis; ensuring that everyone with access to patient-identifiable information is aware of their responsibilities; understanding and complying with the law; and understanding that the duty to share information can be as important as the duty to protect patient confidentiality.
- GDPR, which regulates digital data and places a much stronger emphasis on the clarity and

transparency of communication to the users and introduces the choice of opting out.

- Our own framework for digital disengagement that places opt-out as a starting point of any assessment.

Combining the three, we propose that the following criteria should be used for assessing health apps' Terms and Conditions:

1. What information is said to be collected?
2. How is data stored?
3. What is the app's Privacy Policy?
4. Can patients request to see their data?
5. Is there an opt-out policy? What is included in it?

Applying our criteria to the three apps, we found that the information for each varied greatly in length, clarity and detail. For example, Echo and BH provided minimal explanation about which data was collected, how it was stored, and whether and with whom it might be shared: Echo only stated that they kept the information 'confidential', and BH stated that the information would be shared with GPs and private insurance providers. Neither offered an option to choose which parts of their data the user may decide to share (or not). PTBA, on the other hand, detailed how different types of data (identifiable versus anonymised) were stored and used, and offered an option for opting out of sharing the data with 'affiliates' and partners. The apps also differed substantially when it came to 'Privacy Policy': Echo was the only one offering information on both GDPR and Caldicott in its policy. BH and PTBA, on the other hand, stated that their data was shared with third parties who have their own policies. The responsibility here was placed on the user, who was expected to make decisions about information sharing at their own discretion. BH, in particular, called the users to carefully read those parties' documentations: 'These policies are the policies of our third-party service providers. As such we do not accept any responsibility or liability for these policies.'⁷

While the first three criteria refer to collecting, storing and sharing information *in* and *by* the apps, we were also particularly interested in contexts where the users may wish to take their data *out* of the apps – whether by requesting access to it and/or by opting out. Both of those steps seem to appear complicated, and in some cases, impossible. Echo allowed withdrawal of consent within a set time frame; PTBA stated that one could opt out from marketing communications as well as from sharing personal information with affiliates and third parties, and could contact the company with requests to 'review, correct, update, restrict or delete' personal information.⁴² BH, on the other hand, did not allow any opt-out at all, apart from

receiving marketing materials. Finally, although our apps allowed users to access their data, Echo and BH charged a fee for any information request. At the same time, these opt-out options applied only to new forms of data collection. When a user opts out of certain forms of data sharing, or deletes their account, information that has already been obtained (including sensitive data, such as fertility of HIV status) might remain and will continue to be used by the app or the third parties. For example, PTBA policy stated: 'Please note that if you opt out as described above, we will not be able to remove your personal information from the databases of our affiliates with which we have already shared your information (i.e. as of the date that we implement your opt-out request)'.⁴² BH's Terms and Conditions stated that not all data could be deleted and thus in case of deactivation, some data will continue to be used, in anonymous forms, for research. Most worryingly, it is unclear how this distinction between 'new' and 'already obtained' data is applied during transition periods. Requests to delete personal information or deactivate an account are lengthy (taking an average of 30 days) and conditional, and no guidance is provided about the moment when the data mining ceases.

Mapping apps' data sharing practices

While analysing the health apps' Terms and Conditions reveals the sheer complexity and the conflicting nature of the legal and social frameworks within which health apps exist, it does not necessarily tell us *how* these framework actually operate within the app environment itself. Because apps are embedded in smartphones and operate in connection to other phone features, it is crucial to examine the app's data behaviour in the device environment. Therefore, the second element of our toolkit examines which data is collected and shared by the apps via 'permission' requests and trackers, using what can be described as a 'track the tracker' technique.

The meaning and purpose of 'permission' is described by Android developer documentation as a way to protect personal data when a user accesses an app on their smartphone. While there are many different levels and sub-levels of permission requests within Android applications, for the purposes of this project, we focused on the two most common protection levels that affect the sharing of user data with third-party apps: 'normal' and 'dangerous'. 'Normal' permissions cover areas where an app needs to access data or resources outside of itself, 'but where there is very little risk to the user's privacy or the operation of other apps. For example, permission to set the time zone is a normal permission'.⁴³ 'Dangerous' permissions require sensitive or private user information

(such as phone and email contacts, or text messages), or access to phone features such as camera or automatic calling performed by the app without the user touching a dialler. To use a ‘dangerous’ permission, the app must request agreement from the user when it first runs: for example, by indicating that they accept the Terms and Conditions or Privacy Policy. ‘Dangerous’ permissions can also be ‘malicious’ – a term commonly used in the world of cybersecurity – meaning ‘exploitable’. These are permissions that are required for the app to work, and can remain dormant without ever being taken advantage of. However, if exploited by a cybercriminal, ‘dangerous’ permissions make the user and their data most vulnerable.^{44,45}

Assessing our selected apps in relation to the amount and type of ‘permissions’ they request demonstrates that even when Terms and Conditions present robust privacy policies, the apps themselves draw excessive additional information, beyond the actual purpose of the app for reasons which are neither clear nor justified. Many of these – for example users’ geo locations, phone calls, text messages or phone calls – access and share personal data in unclear and obscure ways that are ethically dubious and can compromise users’ privacy, human/citizen rights and potentially breach GDPR regulations, as summarised in Table 1 below.

To make matters worse, apps also contain a substantial amount of trackers, mining data about the way users use the app, and sharing data with third-party analytics. What is particularly important is to examine trackers and permissions in relation to each other, through for example, the ‘track the tracker’ technique that we implemented with the help of Exodus and Apktool. In order to communicate joint effects of tracking permissions and data sharing, and to facilitate a more comprehensive and nuanced analysis, we developed an interactive data visualisation tool.⁴⁶ This tool enables us to demonstrate the apps’ operation in the smartphones that host them, and reveals ways in which a single health app is embedded in the multi-platform network of data mining and sharing. Figures 1–4 below present screen shots of data output as tested on our three apps.

Mapping and analysing permissions and tracking together demonstrate the importance of addressing not just the quantity but also the specific nature of data tracking. For example, PTBA seems to share the largest amount of data with the most trackers, while Echo has the fewest permissions, and as such, may seem less invasive. However, its permissions request for ‘Access [to] Coarse Location’ feeds one of the most ‘leaky’ combinations of app trackers in terms of the ways in which user data is documented, traded and shared across social networks, and how and when it is

displayed. Like PTBA, Echo uses Facebook trackers, most specifically, Facebook Login (to share login data from the app with Facebook), Facebook Analytics (tracking anonymised, though context and category/theme-based data), Facebook Places (sharing location), and Facebook Share (ability to share health data to other contacts on Facebook). Among all the third-party trackers we documented, the seemingly unassuming tracker entitled ‘GoogleCrashlytics’ may be the most problematic one. It was used by Echo and BH. In addition to reporting to developers whenever an app crashes, or how many times it is used, GoogleCrashlytics allows developers to advertise across various hidden advertising networks, some of which are potentially untraceable beyond Facebook and Google adverts, but with whom sensitive data might be shared.

Passing app data to third parties, cross-referencing data with information from other apps on the phone and combining it with behaviour mining via social media analytics has extensive potential for indirect, yet substantial, intrusion into users’ privacy and confidentiality. One of the ways in which it happens is when sensitive health-related adverts are offered to users based on the app’s sharing of the information regarding GP appointments, medical topics discussed via the app, or prescriptions ordered. These adverts might be particularly unwelcome when they ‘follow’ the user outside the app, breaching what Nissenbaum⁴⁷ describes as the ‘contextual integrity’ of personalised and private data as it is shifted beyond its original (in our case, health-related) sphere of user practice and intention to become a means of digital surveillance. Such ads can pop up on social media, Google, in games or a general browsing, especially if the user’s geolocation presents an opportunity. For example, a user could be ordering a prescription for fertility medication while out shopping, and depending on their location, an advertising network might show them where a pregnancy test kit might be purchased without consideration of where and when a person might be accessing those (at home, work, in a public space, next to a family member), and what the implications of such out-of-app following might be. These potentially unwelcome exposures can affect anyone using a health app, but might be particularly problematic in instances of HIV-related, mental health, or fertility information, which is regarded by many as extremely personal, and as such, is often ferociously guarded. Sharing any health information to Facebook contacts poses similar, if not graver, dangers.

When developing and testing our toolkit on the three apps, we found a range of inappropriate data behaviours, from vague, limited and unclear information about the nature and purpose of data sharing – that is, would it be shared with GPs? The NHS?

Table 1. How ‘dangerous’ permissions can be exploited for ‘malicious’ use by cybercriminals.

Permissions request	What permission does	How permission can be exploited by malicious cybercriminals
Read phone state and identity (android.permission.READ_PHONE_STATE) (android.permission.CALL_PHONE)	Lets app know user is taking calls or is connected to a network. Gives app access to information such as user’s phone number, International Mobile Equipment Identity (IMEI) number, and other identifying information. Apps often use this to identify users without requiring more sensitive information.	Information-stealing malicious apps often target device and phone information.
Access coarse and fine location (android.permission.ACCESS_COARSE_LOCATION) (android.permission.ACCESS_FINE_LOCATION)	Grants access to user’s exact location through the Global Positioning System (GPS), cell sites and Wi-Fi. App developers can gain profit from location-based ads.	The app can know where a user is at all times. Malicious cybercriminals can hack an app and use these permissions to load location-based attacks or malware, or let burglars know when a user is far away from home.
Full Internet access (android.permission.INTERNET)	Apps can connect to the Internet.	Malicious apps use the Internet to communicate with their command centres or download updates and additional malware.
Modify/delete SD card contents (android.permission.WRITE_EXTERNAL_STORAGE)	This lets apps write on external storage, like SD cards.	Cybercriminals use this to store copies of stolen information or save files onto a user’s SD card before sending them to a command centre. Malicious apps can also delete photos and other personal files on a user’s SD card.
Camera (android.permission.CAMERA)	This lets the app use your phone to take photos and record videos <i>at any moment</i> .	Cybercriminals can use this feature as a visual recording device to take pictures/videos of targeted parties (e.g. general users/celebrities/politicians)
Record audio (android.permission.RECORD_AUDIO)	An app can record <i>ALL</i> of a user’s conversations. Not only when a user is speaking on the phone, but all day long.	Cybercriminals can use this feature as a listening device to record conversations of targeted parties (e.g. general users/celebrities/politicians).

Medical research? Private non-medical companies? Which and for what purpose? – to potential direct violations of both the Caldicott and GDPR principles. As we have demonstrated, such behaviours appeared in various combinations in the three apps. Our aim, however, was not to determine which of the three did ‘better’ or ‘worse’, nor even to see whether the apps aligned with user expectations, as understanding the latter would require a separate study. Rather, our discussion points out that data violations is not a binary category of compliance/non-compliance, but a continuum. We propose that our toolkit might be particularly

useful to inform further studies of this continuum, on which a larger number of studied apps could be placed.

Documenting the steps needed to delete an app and withdraw data

One might argue that data collected via apps’ permissions is given by users voluntarily; furthermore, it may seem that users have a degree of control by withholding certain permissions. However, this does not fully allow an opt-out of data aggregation. Although it is possible to restrict some permissions via the smartphone

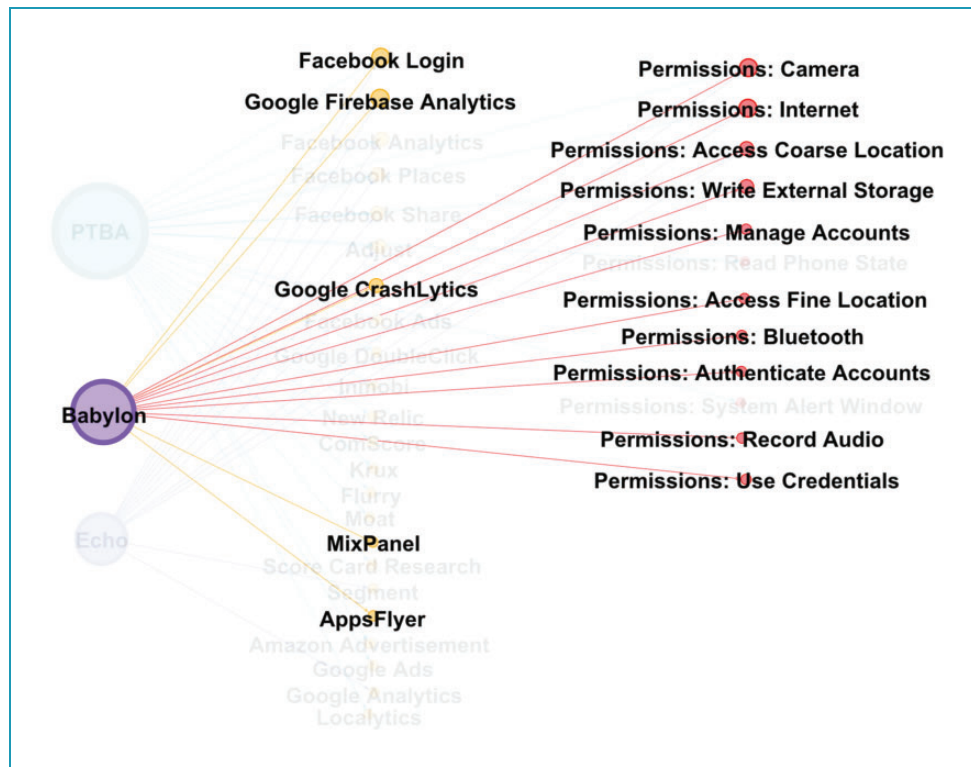


Figure 1. Babylon Health app: User trackers + app permission requests.

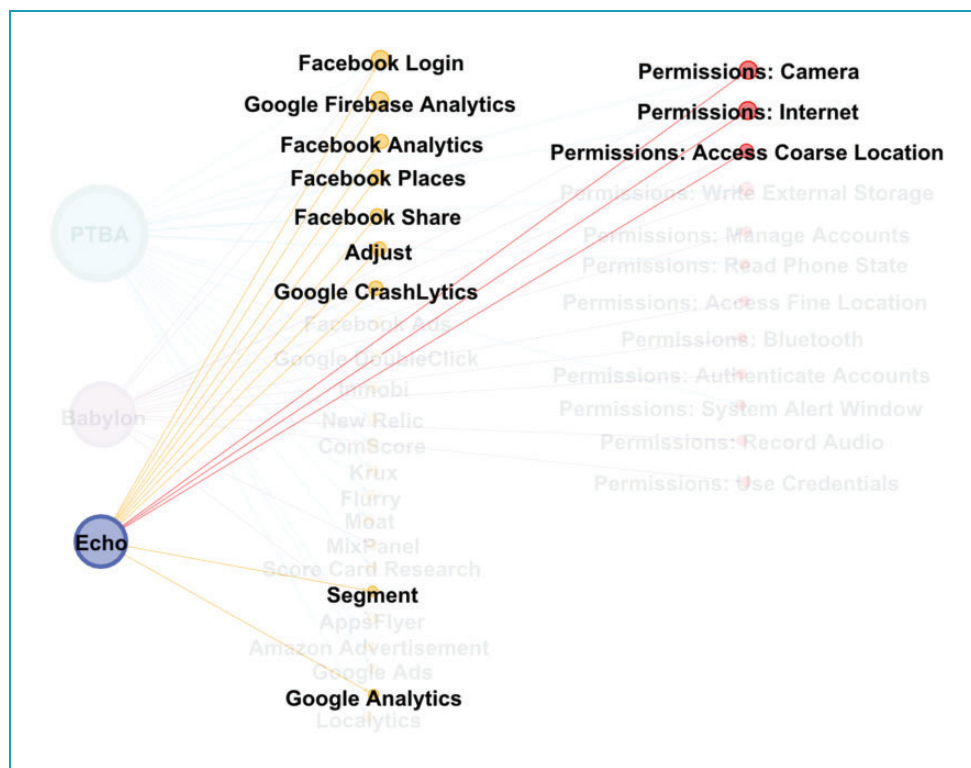


Figure 2. Echo app: User trackers + app permission requests.

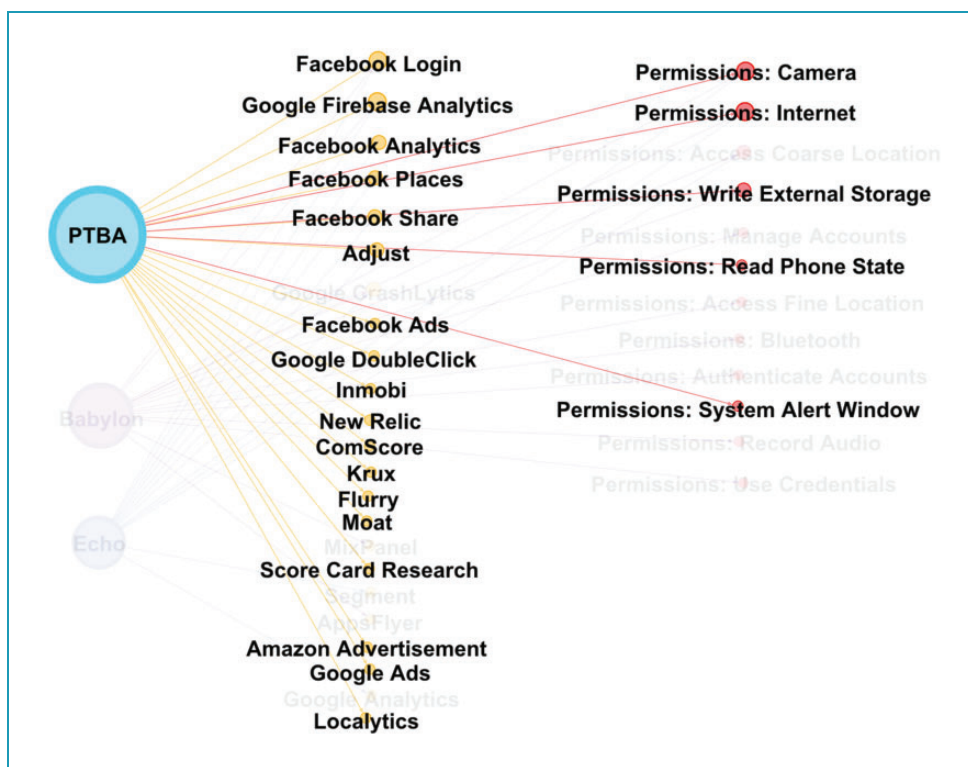


Figure 3. Pregnancy Tracker & Baby App: User trackers + app permission requests.

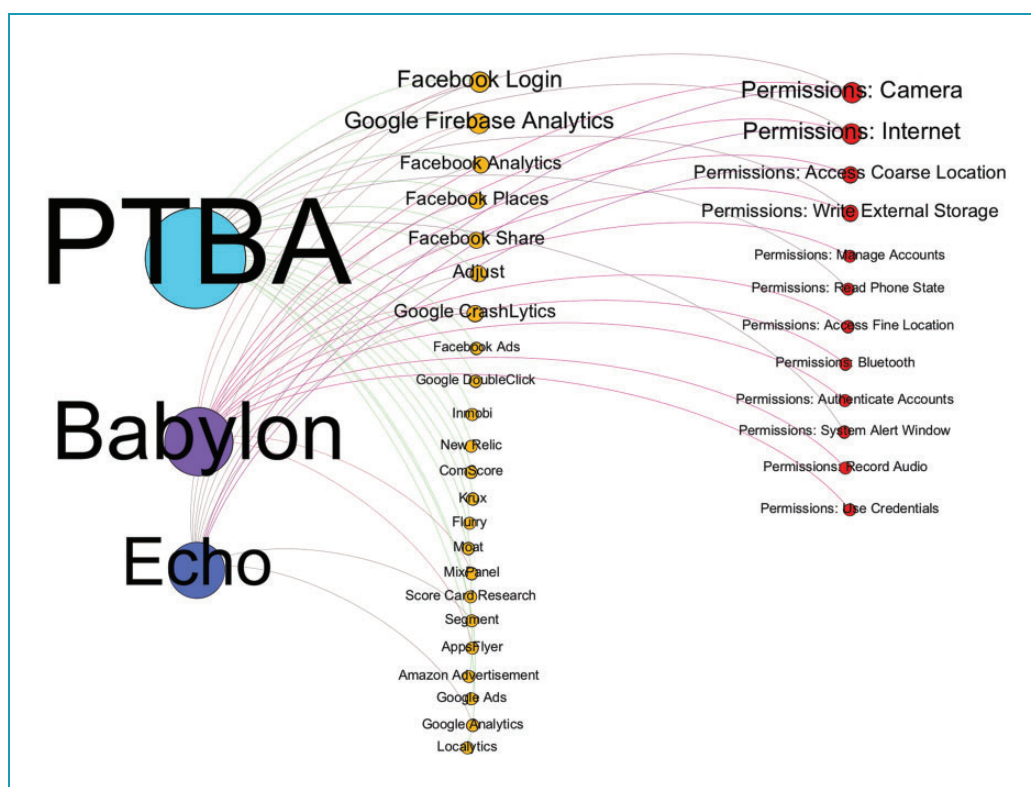


Figure 4. Babylon Health, Echo and Pregnancy Tracker & Baby App apps: Collective user tracking and permissions requests.

settings, when going back to the app, the user receives warnings that core features are no longer accessible, and restoration of permissions is required for the app to function properly. The other option is to discontinue/uninstall the app entirely. However, as both our evaluation of Terms and Conditions and the tracking of the apps' sharing and storage capabilities suggest, removing the app does not necessarily stop the data aggregation and mining, or does so only partially. The final component of our toolkit is therefore dedicated to documenting the step-by-step process of opting out, according to the following criteria:

1. How easy it is to do so within the app?
2. How long does the process take?
3. What are the types of data one can or cannot opt out of?

Of the three apps, Echo offered the most clear and streamlined process, where the deletion of an account was accompanied by clearly labelled screens from within the app (see figures 5–6). Echo was also most clear and transparent about the time frame of the process, and the totality of deletion. After asking the user to confirm that they did indeed want to delete their data, Echo followed through by informing the user that within the GDPR advised 'reasonable' period for deleting user data', it aimed to remove all the user's data at their request, within 30 days.

The other two apps (BH and PTBA) were far less straightforward. PTBA, for example, did not provide an easy way for the user to opt out of sharing their data, despite having detailed (albeit contradictory) information on opt-out options in their Terms and Conditions. When attempting to delete the account, the user was directed to the 'FAQ' link, accessible via

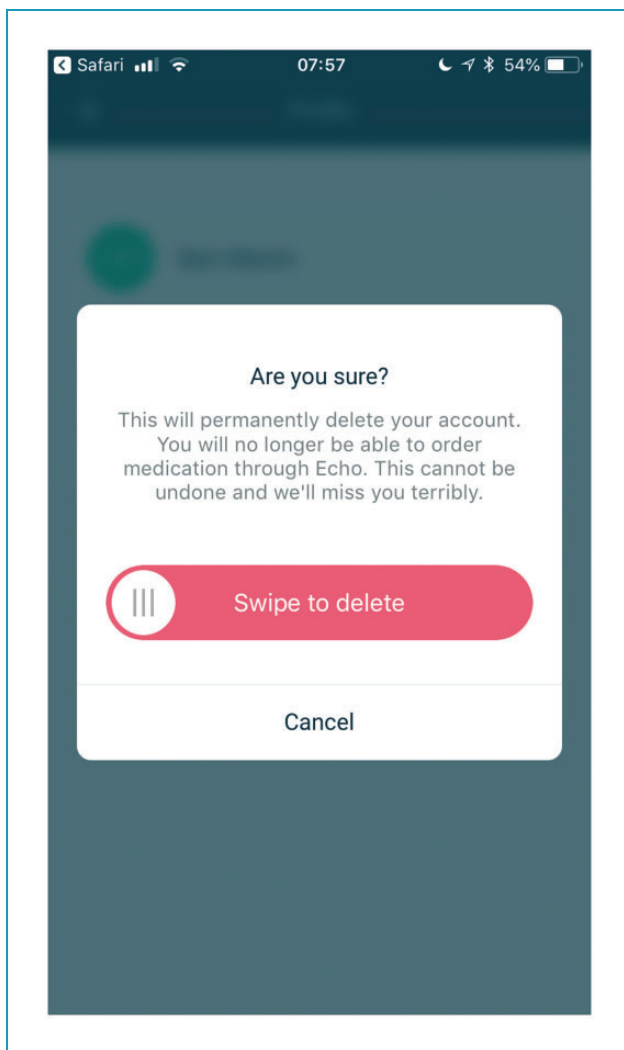


Figure 5. Echo app: deleting the account.

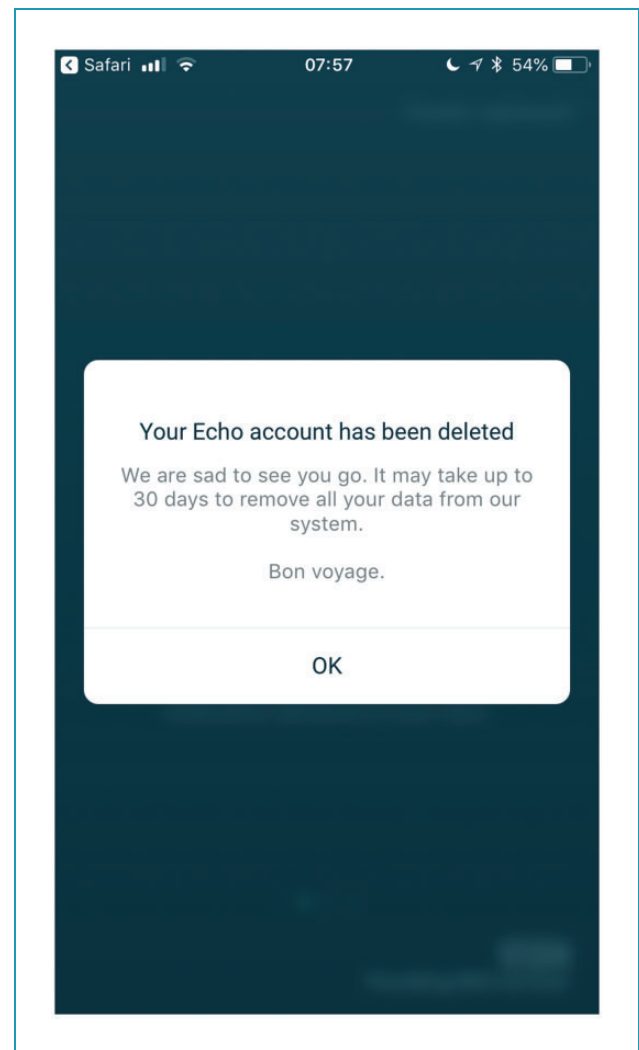


Figure 6. Echo app: deleting the account.

the 'More' menu; however the only opt-out option available was to remove the baby registered for development monitoring, as part of the app's use. Instead of having the option to delete their account or opt out of sharing their data, users had to resort to: '10. My question about the app isn't answered here. Where can I get more help?', which guided them to contact the UK support services to discuss alternatives (Figure 7).³⁵ Similarly, despite having a clearly presented Privacy Policy, BH offered no direct way of opting out of data sharing, or deleting the account entirely from within the app. Again, one needed to go through a similar 'Help' option in the 'Settings' menu only to be redirected to the app's website (Figure 8) for information on cancelling different subscription levels, and the account itself. Worryingly, as of 12 July 2018, despite the implementation of the GDPR, BH still incorporates the less thorough Data Protection Act 1998 in terms of handling requests for cancellation.

In neither case was the time frame for the process clear, nor was there a guarantee of which data would be removed.

Our assessment of BH's and PTBA's opting out procedures suggests that these are made cumbersome-by-design, whether on a practical interface level or in terms of legal specificities. The labour and responsibility of finding a way out is placed on the user: in the case of BH, the user was required to navigate numerous 'Help' screens, and individually cancel each aspect of their membership/use/subscription to the different services within the app. In the case of PTBA there was no direct way of removing the data from within the app. Instead, the user had to read through lengthy pages of the Terms and Conditions and Privacy Policy that had been set out to cover both the app and the website communities used by users. Subsequently, the user had to fill in a form where the only choice for opting out of sharing one's data was to choose the

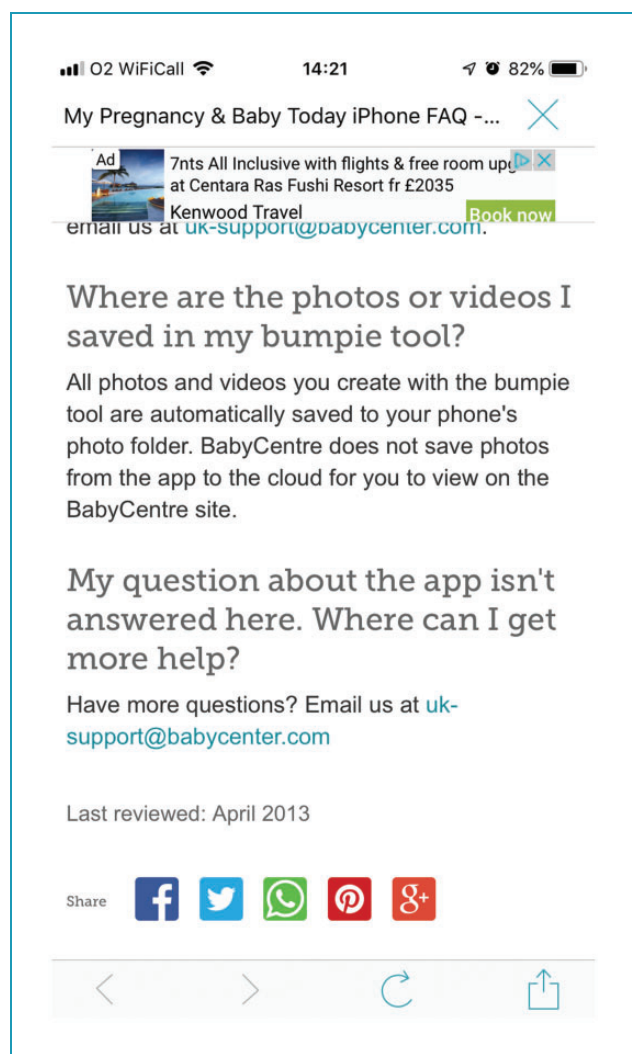


Figure 7. PTBA app: No direct opt-out from app.

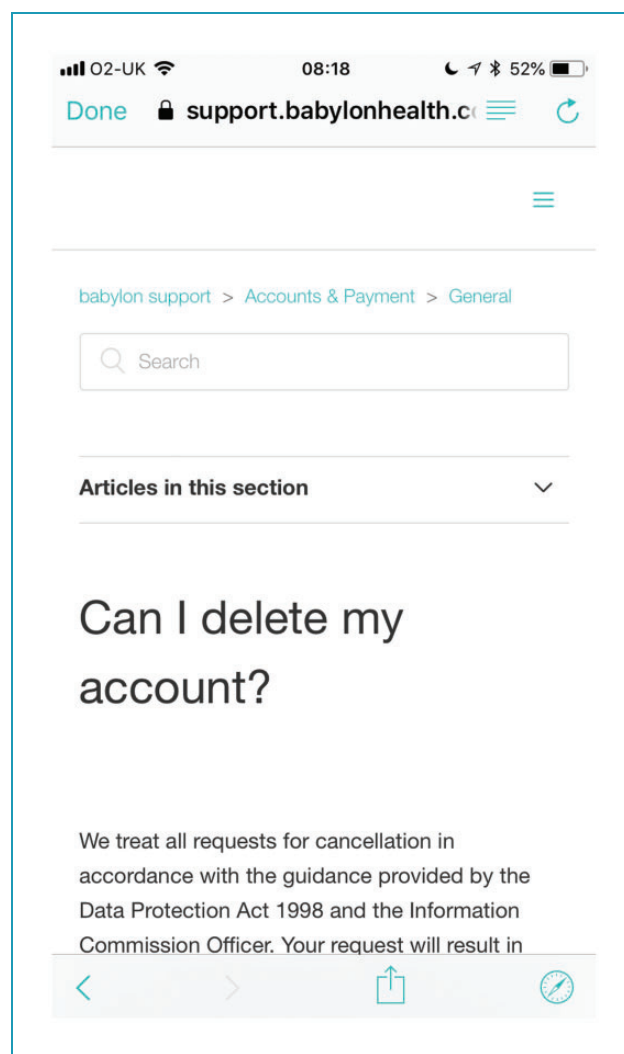


Figure 8. Babylon app: Deleting the account.

drop-down selection, ‘Data protection questions’, and then try to explain in a free text form that they would like to have their data removed. The user was also made responsible for looking into any third-party apps the PTBA software may have shared the data with, and extricate it accordingly. All these tasks require a high degree of technical knowledge and legal literacy, which most users do not possess. In other words, neither having rigorous Terms and Conditions nor providing a clear interface options are sufficient, on their own, to facilitate a straightforward and readily available opt-out process. While email support or a ‘delete your account’ button within an app may *promise* an easy fix, the reality of opting out of data, once a person has started using the app, is complicated and uncertain.

Conclusion

Our analysis of health appisation in the UK reveals the currently heightened national concerns over personal data management within the context of GDPR and the wider changes in European data policies. One could argue that the move to become ‘GDPR-compliant’ is a step towards data justice and increased digital rights of users/patients, where opting out is becoming institutionalised. Yet a closer look at how such compliancy is being implemented – not just through everyday practices, but also at a more granular and algorithmic level of health apps – reveals a fluid and complex web of networked ‘data traps’ that act as resource nodes of biodata. These ever-changing and often contradictory settings in the contemporary UK–European socio-economic, legal and political landscape rely on their data subjects to be digitally engaged, or (un)willing participants in the process of the digitisation and appisation of health. Practices and technologies of opting out struggle to find a place within such a context that is simultaneously part of the global capitalist data economy where opt-out rights are diminishing and personal data is shared easily, *and* is subject to new data protection regulation that places opt-out rights at its centre.

Emerging directly from conflicting civil, clinical and corporate frameworks surrounding personal data usage is a further tension that manifests very specifically within the area of digital health. The process of appisation, which is based on having an *individual* gadget and an *individual* account to support one’s needs, signals the increasing self-responsibilisation of health: self-care, self-management, self-tracking and self-monitoring.^{5,48–52} On the one hand, then, digital health is about the individual, where responsibility and accountability of one’s own health now includes responsibility for one’s own personal data; as we have shown throughout our analysis, the onus of finding,

safeguarding, accepting, refusing, and figuring ways out is always on the individual user. Furthermore, the management of one’s data is often presented with an *illusion of choice*. This is particularly apparent in how the NHS Apps Library interpellates the ‘you’ and the ‘self’⁵³ in practices such as accepting Terms and Conditions, or in granting app permissions, not to mention the very decision to choose and install an app – the epitome of agentic ‘consumer choice’.^{54–56} On the other hand, as our ‘tracking the tracker’ technique has consistently demonstrated, health apps bring a radically new level of data powerlessness. When health information is shared, and jointly mined, with a search/advertising engine (Google) or a social networking site (Facebook), the idea of ‘doctor–patient confidentiality’ becomes all but a symbolic gesture from bygone days. Health appisation gives rise to algorithmic ‘care’, one based on analytics that might be more efficient, speedy and precise yet also relentlessly intrusive and non-private, where no medical information is left untouched, unseen, undisclosed.

Crucially, the broad and extensive sharing of our personal (bio)data for analytics and profit means that opting out, or the use, of health apps is first and foremost about large-scale dataisation and the economy of surveillance capitalism.⁵⁷ While data management practices are individual, and targeted advertising is also individually tailored, the individual is meaningless in the eyes of algorithmic determinism and prediction. A single user’s data has no representative value: monetary and statistic capital lies with the aggregated *Big Data*. It is at this tension that the digitisation of health lies, between the neoliberal model of the individual whose health and data concerns are personalised into the ‘Self’, and the digital-capitalist model,^{58–61} which generates value from the collective, and is thus representationally and statistically ‘valid’ – the data of the masses. It is here that we witness what Btihaj Ajana coined the shift ‘from individual data to communal data, from the Quantified Self to the ‘Quantified Us’, from the ‘biopolitics of the self’ to the biopolitics of the population’⁴⁹ (p. 14).

Within such a context, ‘opting out’ is pulled across oppositional forces: it is a matter of individual rights (and responsibilities), while also, paradoxically, situated within a system that supports, and capitalises on, *mass* value and *mass* data. Legal changes such as the GDPR are undoubtedly a welcome and much needed attempt to protect individual rights in the world of large-scale data sharing, mining and profiling. Yet, in addition to exploitable legal loopholes (such as the out-of-app Terms and Conditions) within supposedly GDPR-compliant apps there are also technical loopholes (as we have seen through various ‘permissions’ pinned to optimal app functionality) that work

together in complicit ways that endanger the individual. The combination of legal and technical loopholes needs to be exposed and amended, because herein a more substantial issue is at stake in relation to the effectiveness of legal frameworks such as GDPR. When the digital data economy traffics in Big Data, and when, as a result, individual data ownership erodes in favour of ‘data philanthropy’ – a growing shift towards ‘surrendering’ one’s data for the ‘public good’, where unwillingness to share and concerns for privacy are seen as ‘selfish and anti-solidaristic’⁴⁹ (p. 11) – legally addressing *individual* responsibility and *individual* protection is not enough, and will never be fully efficient. How, then, can we approach, analyse and change the current landscape of the ‘socio-cultural data traps’ of health apps?

First and foremost, we require a further, more extensive and more nuanced understanding, mapping and monitoring of the dataised operation of health apps. This is where we see the main methodological and practical impact and value of our proposed toolkit, offered here for further development and use by others, in both social research and healthcare provision. While we tested and developed our toolkit in the UK, its key principles can be rescaled and adjusted to use elsewhere. The power of our toolkit is twofold: it allows the identification of loopholes and ‘vulnerabilities by design’ within the apps, as well as fleshing out discrepancies between data policies and data practices. Only when we can ‘see’ the differences between the individualised discourse of health apps as they present themselves, and the inner workings of data extraction, can we begin to understand the complexities of digital health’s data traps. The open source platforms we used are widely available and in themselves are not new. But it is in using them in conjunction with the discursive analyses of the apps’ websites and their Terms and Conditions *and* of the institutional socio-legal frameworks in operation, that one can begin to build a fuller picture and understanding of what the digitisation and appisation of health entails, and how it operates on both an individual and collective level.

Secondly, we must also rethink the idea of ‘data rights’ in digital health, by shifting towards the perspective of data *justice*, and this is where we see our article’s main theoretical contribution to the field of critical digital health scholarship. By introducing opt-out as a conceptual lens and as a starting point of our critical inquiry, we are calling to denaturalise digital engagement itself when discussing the relations between health and everyday communication technologies. Our proposed paradigmatic shift towards digital *dis*-engagement should not be understood as a call to abandon all apps or other digital technologies, or turn towards technologically free healthcare. Rather, we offer a way for a

critical and sceptical assessment of health apps – and more broadly, of other digital communication technologies – as they are being introduced and adopted, beyond their clinical effectiveness or their potential to save human resources in healthcare. Such assessment must include, but also go beyond, individualised solutions such as raising awareness or legally protecting individual user’s rights. In order to create a space for both individual rights to refuse to be part of a database,¹⁴ and a more systemic, collective refusal of ‘biopolitical categorisations that are enabled through Big Data practices’⁴⁹ (p. 13), we need to move away from the biopolitics of commodification to a true commitment to health and care. To do that, opting out needs to be our ethical anchor and our starting point.

Acknowledgements: The authors would like to thank the Manchester Metropolitan University student intern Edward Johnson, for his dedicated assistance with collecting and overviewing data about the National data opt out service by NHS Digital. We are grateful to EJ Gonzalez-Polledo for their insightful comments on the earlier draft of the manuscript. We also thank the two reviewers for their helpful suggestions and guidance in preparing the final version of the manuscript.

Contributorship: AK and EM conceived the conceptual framework of the study. SM developed the protocol of assessing the apps’ data and designed the data visualisation tool. All authors reviewed and analysed different areas of findings according to expertise. AK and EM prepared the initial draft of the manuscript; all authors consequently edited and approved the final version of the manuscript.




Conflict of interests: The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Ethical approval: The Arts and Humanities Research Ethics and Governance Committee, Manchester Metropolitan University approved this study on 18 April 2018 (internal reference number: 0603).

Funding: The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This work was supported by the British Academy/Leverhulme Small Grant (Grant no. SG170293).

Guarantor: AK

ORCID iDs

Adi Kuntsman  <https://orcid.org/0000-0002-9970-9866>
Esperanza Miyake  <https://orcid.org/0000-0001-5504-7648>
Sam Martin  <https://orcid.org/0000-0002-4466-8374>

Peer review: This manuscript has been reviewed by Dr. Linnet Taylor, Tilburg University and Dr. Pepita, Hesselberth, Leiden University Centre for the Arts in Society.

References

- Gardner H and Davis K. *The app generation: how today's youth navigate identity, intimacy, and imagination in a digital world*. Yale: Yale University Press, 2013.
- Miller PD and Matviyenko S. *The imaginary app*. Cambridge and London: MIT Press.
- Morris JW and Murray S. *Appified: culture in the age of apps*. Michigan: University of Michigan Press.
- Statista: The Statistics Portal. mHealth: statistics and facts, <https://www.statista.com/topics/2263/mhealth/> (accessed 1 October 2018).
- Lupton D. Apps as artefacts: towards a critical perspective on mobile health and medical apps. *Societies* 2014; 4: 606–622.
- Van Dijck J and Poell T. Understanding the promises and premises of online health platforms. *BD&S* 2016; 3: 1–11.
- Babylon Health, <https://www.babylonhealth.com/> (accessed 12 December 2018).
- Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization. *J Inf Technol* 2015; 30: 75–89.
- Cinnamon J. Social injustice in surveillance capitalism. *Surveillance Soc* 2017; 15: 609–625.
- Lehtiniemi T. Personal data spaces: an intervention in surveillance capitalism? *Surveillance Soc* 2017; 15: 626–639.
- Silverman J. Privacy under surveillance capitalism. *Soc Res* 2017; 84: 147–164.
- Johnson J. From open data to information justice. *Ethics Inf Technol* 2014; 16: 263–274.
- Dencik L, Hintz A and Cable J. Towards data justice? The ambiguity of anti-surveillance resistance in political activism. *BD&S* 2016; 3: 1–12.
- Taylor L. (2017) What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society* 2017; 4(2): 1–14.
- Iliadis A. Algorithms, ontology, and social progress. *Glob Media Commun* 2018; 14: 219–230.
- Kuntsman A and Miyake E. The paradox and continuum of digital disengagement: denaturalising digital sociality and technological connectivity. *Media Cult Soc* 2019; 41: 901–913.
- Oborn E and Barrett S. Digital health and citizen engagement: changing the face of health service delivery. *Health Serv Manag Res* 2016; 29: 16–20.
- Scherer EA, Ben-Zeev D, Li Z, et al. Analyzing mHealth engagement: joint models for intensively collected user engagement data. *JMIR mHealth uHealth* 2017; 5: e1.
- Kanstrup AM, Bertelsen P and Jensen MB. Contradictions in digital health engagement: an activity tracker's ambiguous influence on vulnerable young adults' engagement in own health. *Digit Health* 2018; 4: 1–13.
- Long MW, Albright G, McMillan J, et al. Enhancing educator engagement in school mental health care through digital simulation professional development. *J School Health* 2018; 88: 651–659.
- Light B, Burgess J and Duguay S. The walkthrough method: an approach to the study of apps. *New Media Soc* 2018; 20: 881–900.
- Elenko R, Speier A and Zohar D. A regulatory framework emerges for digital medicine: clear and logical regulatory guidelines on the process and requirements for approval of health apps and wearable sensors will be essential for the digital medicine sector to unleash its full potential. *Nat Biotechnol* 2015; 33: 697–702.
- Hsu JM. Digital health technology and trauma: development of an app to standardize care. *ANZ J Surg* 2015; 85: 235–239.
- NHS Digital, <https://digital.nhs.uk/> (accessed 1 June 2018).
- Lucas H. New technology and illness self-management: potential relevance for resource-poor populations in Asia. *Soc Sci Med* 2014; 145: 145–153.
- Morton K, Dennison L, May C, et al. Using digital interventions for self-management of chronic physical health conditions: a meta-ethnography review of published studies. *Patient Educ Couns* 2016; 100: 616–635.
- EU GDPR. GDPR key changes, <https://www.eugdpr.org/key-changes.html> (accessed 1 June 2018).
- NHS Digital. National data opt out, <https://digital.nhs.uk/services/national-data-opt-out-programme> (2018, accessed 1 June 2018).
- NHS Digital. NHS Apps Library, <https://digital.nhs.uk/services/nhs-apps-library> (accessed 5 June 2018).
- NHS Digital. NHS Apps Library Beta version, <https://apps.beta.nhs.uk/about-us/> (accessed 27 June 2019).
- Digital Assessment Questions: Beta, <https://developer.nhs.uk/digital-tools/daq/> (accessed 30 July 2018).
- Echo, <https://www.echo.co.uk/> (accessed 12 December 2018).
- babycentre, <https://www.babycentre.co.uk/mobile-apps> (accessed 12 December 2018).
- Babylon GP at hand, <https://www.gpathand.nhs.uk> (accessed 12 December 2018).
- babycentre. Pregnancy Tracker & Baby App, <https://play.google.com/store/apps/details?id=com.babycenter.pregnancytracker> (2018, accessed 2 July 2018).
- Github, <https://github.com/Exodus-Privacy/exodus> (2018, accessed 1 June 2018).
- Doctorow C. Researchers craft Android app that reveals menagerie of hidden spyware; legally barred from doing the same with iOS, <https://boingboing.net/2017/11/25/la-la-la-cant-hear-you.html> (2017, accessed 29 March 2018).
- Exodus privacy, <https://exodus-privacy.eu.org/> (2018, accessed 29 April 2018).
- Zang J, Dummit K, Graves J, et al. Who knows what about me? A survey of behind the scenes personal data sharing to third parties by mobile apps, <http://techscience.org/a/2015103001> (2015, accessed 15 October 2019).
- Apktool, <https://ibotpeaches.github.io/Apktool/> (2018, accessed 20 April 2018).
- NHS Digital. Caldicott Principles, <https://www.igt.hscic.gov.uk/Caldicott2Principles.aspx> (accessed 1 January 2019).

42. babycentre. Privacy policy, <https://www.babycentre.co.uk/e7814/privacy-policy> (2018, accessed 2 July 2018).
43. Android Developers. Guides: permissions overview, <https://developer.android.com/guide/topics/permissions/overview#permissions> (2018, accessed 29 March 2018).
44. Trend Micro. 12 most abused Android app permissions, <http://about-threats.trendmicro.com/us/library/image-gallery/12-most-abused-android-app-permissions> (2018, accessed 22 July 2018).
45. Kaspersky Lab. All about Android app permissions, <https://www.kaspersky.com/blog/android-permissions-guide/14014/> (2017, accessed 22 July 2018).
46. Rethinking Digital Health Opt-Out: Smartphone Trackers, digitalcoeliac.com, <http://www.digitalcoeliac.com/rethink-dh2018> (accessed: 12 December 2018).
47. Nissenbaum H. Privacy as contextual integrity. *Washington Law Review* 2004; 79: 119.
48. Lupton D. Digitized health promotion: personal responsibility for health in the Web 2.0 era. *UNSW Sydney*, https://www.researchgate.net/publication/237608665_Digitized_health_promotion_personal_responsibility_for_health_in_the_Web_20_era (2013, accessed xx Month Year).
49. Ajana B. Digital health and the biopolitics of the quantified self. *Digit Health* 2017; 3: 1–18.
50. Neff G and Nafus D. *The self-tracking*. Massachusetts: MIT Press, 2016.
51. Sharon T and Zandbergen D. From data fetishism to quantifying selves: self-tracking practices and the other values of data. *New Media Soc* 2017; 19: 1695–1709.
52. Kristensen DB and Ruckenstein M. Co-evolving with self-tracking technologies. *New Media Soc* 2018; 20: 3624–3640.
53. Althusser L. *Lenin and philosophy, and other essays*. New York: Monthly Review Press, 1971[2001].
54. Borgerson J. Materiality, agency, and the constitution of consuming subjects: insights for consumer research. In: Menon G and Rao AR (eds) *NA – advances in consumer research*, vol. 32. Duluth, MN: Association for Consumer Research, 2004, 439–443.
55. Bauman Z. *Consuming life*. Cambridge: Polity Press, 2007.
56. Schwarzkopf S. Consumer-citizens: markets, marketing, and the making of ‘choice’. In: Kravets O, Maclaran P and Miles S (eds) *The SAGE handbook of consumer culture*. London: SAGE Publications, 2018, pp. 435–452.
57. Zuboff S. Big other: surveillance capitalism and the prospects of an information civilization. *J Inf Technol* 2015; 30: 75–89.
58. Schiller D. *Digital capitalism: networking the global market system*. London and Massachusetts: MIT Press, 2000.
59. Fuchs C. Labor in informational capitalism and on the internet. *Inf Soc* 2010; 26: 179–196.
60. Fuchs C. *Digital labour and Karl Marx*. London: Routledge, 2013.
61. Fuchs C. *Culture and economy in the age of social media*. New York, London: Routledge, 2015.